THE NECESSITY OF CYBER INNOVATION

Federal agencies are being offered a wealth of ideas and advice for shoring up cyber defenses.

The White House and Congress are both looking for new ideas to address long-standing cybersecurity concerns in the federal government, and some old ideas are drawing renewed interest. The new administration put its stamp on the issue with a May 11 executive order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." This long-awaited order seeks to bolster cyber efforts by both mandating enterprise risk management and mitigation practices and reiterating the need for modernization of agency IT infrastructures.

The executive order has become part of a broader conversation about how agencies can raise the bar on cybersecurity. Modernization is a central part of that, because legacy systems are increasingly costly and difficult to protect—but that's only part of the solution.

STRENGTHENING CYBER DEFENSES

Here is a roundup of some of the latest ideas being championed by federal IT officials, cyber experts, and congressional leaders.

THE CYBERSECURITY FRAMEWORK: TIME TO STUDY UP

The Cybersecurity Framework—technically called the Framework for Improving Critical Infrastructure Cybersecurity—is not new. It was released by the National Institute of Standards and Technology (NIST) in 2014. It is, however, getting renewed attention thanks to the recent executive order.

The executive order directs agencies to implement the framework—and to detail their plans for doing so—as part of one of the first mandated reports. The framework was originally developed to help organizations take a risk-management-based approach to managing critical infrastructure. However, NIST officials have said all along that the framework dovetails nicely with its other security and privacy risk-management guidelines.

With that in mind, NIST recently released draft implementation guidance, which outlines different ways in which the framework can strengthen cybersecurity efforts—such as managing cybersecurity requirements, integrating and aligning cybersecurity and acquisition processes, and evaluating cybersecurity from an organizational perspective.

MULTIFACTOR AUTHENTICATION: JUST A MATTER OF TIME

Cyber experts have been saying for years that when it comes to protecting sensitive systems or data, agencies should not rely on the old-school computer password—at least not by itself. "It's hard to find a major cyberattack over the last five years where identity—generally a compromised password—did not provide the vector of attack," according to a February 2017 report from the Chertoff Group titled, "Strong Authentication in Cyberspace."

The problem is hackers have numerous tools they can use to compromise a password without anyone knowing. Multifactor authentication makes it tougher, requiring a user to provide a second form of identification, such as a fingerprint, a smart card, or some other token they must have in hand.

The DoD made the leap years ago, with its adoption of the Common Access Card. A growing number of civilian agencies are taking an interest as well, including the Social Security Administration, the Office of Personnel Management, and the Library of Congress.

Cover: Shutterstock.com

BUG BOUNTY PROGRAMS:
CROWDSOURCED TROUBLESHOOTING

During the last year, the Defense Department has been doubling down on the idea of organizing "bug bounty" contests. These involve inviting so-called white-hat hackers to probe systems for potential weaknesses. As with any crowdsourcing effort, a bug bounty program is seen as a way to give an organization quick access to the energy and talents of outside enthusiasts—people who otherwise might never work on government programs in any formal way.

It's also a matter of quantity. The more people involved in seeking out vulnerabilities, the more likely such vulnerabilities will be found. The Pentagon, Army, and Air Force each have run bug bounty programs in the last year. The Air Force took the concept a step further by making it a global effort, inviting participants from Canada, the United Kingdom, New Zealand, and Australia.

CYBER WORKFORCE:
LOOKING FOR NEW RECRUITS

Bug bounty programs serve their purpose, but they do nothing to address the larger problem—the federal government's perpetual lack of in-house cyber experts. As part of its 2017 high-risk list, the Government Accountability Office (GAO) called for the federal government to step up its efforts to recruit and retain a qualified cybersecurity workforce.

Rep. Will Hurd (R-Texas), chair of the House Oversight Subcommittee on Information Technology, has an idea of how to do this. Instead of hiring cyber experts for permanent positions, he suggests creating a cyber national guard who could serve both the public and private sectors on a rotational basis.

Hurd, along with Rep. Ruben Gallego (D-Ariz.), first pitched this idea at the 2016 SXSW Interactive Festival. He brought it up again at a hearing in June.

INFORMATION SHARING:
CLEARING OUT THE CHANNELS

This is a perennial question—when the federal government discovers vulnerabilities in popular IT products, should it share that information with the private sector? On the one hand, federal officials acknowledge the value of exchanging intelligence with the private sector. On the other hand, they also see the value of classifying that information, with hopes of keeping it out of the wrong hands.

At a June 15 congressional hearing, former U.S. Chief Information Security Officer Gregory Touhill stated the government's "over-classification" of cyber intelligence was the single biggest obstacle to information sharing between the public and private sectors. Such collaboration is seen by Touhill and other cyber experts as key to responding to zero-day events, such as the recent WannaCry ransomware event.

CYBER SHARED SERVICES:
NO NEED TO GO IT ALONE

In the months leading up to the executive order on cybersecurity, federal cyber experts were intrigued by one particular provision being floated—a shared services approach to cybersecurity. The federal government has been pushing the concept of shared services for years, encouraging agencies to share the cost of developing and managing common business functions; such as financial management, human resource management, and acquisition.

The final executive order ups the ante, directing agencies to "show preference in their procurement for shared IT services," particularly when it comes to email, cloud, and cybersecurity. Trump administration officials believe that the shared services model could be a boon for smaller agencies lacking the budget and workforce needed to develop and maintain adequate cyber defenses.